JOHN O'GRADY
CLERK OF THE FRANKLIN COUNTY COMMON PLEAS COURT, COLUMBUS, OHIO 43215
CIVIL DIVISION

TRACY L. KEY INDV
20415 ALPINE DRIVE
LAWRENCEBURG, IN 47025-0000,

PLAINTIFF,

VS.

DSW INC
% CSC-LAWYERS INC SBC
SUITE 1800
50 W BROAD STREET
COLUMBUS, OH 43215-0000,
DEFENDANT.

06CVH-05-6041
CASE NUMBER

RECEIVED
MAY 18 2006
LEGAL DEPARTMENT

**** SUMMONS ****

05/05/06

TO THE FOLLOWING NAMED DEFENDANT:
DSW INC
% CSC-LAWYERS INC SBC
SUITE 1800
50 W BROAD STREET
COLUMBUS, OH 43215-0000

YOU HAVE BEEN NAMED DEFENDANT IN A COMPLAINT FILED IN FRANKLIN COUNTY COURT OF COMMON PLEAS, FRANKLIN COUNTY HALL OF JUSTICE, COLUMBUS, OHIO,
BY: TRACY L. KEY INDV
20415 ALPINE DRIVE
LAWRENCEBURG, IN 47025-0000,

PLAINTIFF(S).

A COPY OF THE COMPLAINT IS ATTACHED HERETO. THE NAME AND ADDRESS OF THE PLAINTIFF'S ATTORNEY IS:
ELIZABETH J. WATTERS
CHESTER,WILLCOX & SAXBE
65 EAST STATE STREET
SUITE 1000
COLUMBUS, OH 43215-4213

YOU ARE HEREBY SUMMONED AND REQUIRED TO SERVE UPON THE PLAINTIFF'S ATTORNEY, OR UPON THE PLAINTIFF, IF HE HAS NO ATTORNEY OF RECORD, A COPY OF AN ANSWER TO THE COMPLAINT WITHIN TWENTY-EIGHT DAYS AFTER THE SERVICE OF THIS SUMMONS ON YOU, EXCLUSIVE OF THE DAY OF SERVICE. YOUR ANSWER MUST BE FILED WITH THE COURT WITHIN THREE DAYS AFTER THE SERVICE OF A COPY OF THE ANSWER ON THE PLAINTIFF'S ATTORNEY.

IF YOU FAIL TO APPEAR AND DEFEND, JUDGMENT BY DEFAULT WILL BE RENDERED AGAINST YOU FOR THE RELIEF DEMANDED IN THE COMPLAINT.

JOHN O'GRADY
CLERK OF THE COMMON PLEAS
FRANKLIN COUNTY, OHIO

BY: SANDY THOMAS, DEPUTY CLERK

(CIV370-S03)

EXHIBIT 1

JOHN O'GRADY
CLERK OF THE FRANKLIN COUNTY COMMON PLEAS COURT, COLUMBUS, OHIO 43215
CIVIL DIVISION

JUDGE D. CAIN

TRACY L. KEY INDV,

PLAINTIFF,

VS.

DSW INC,

DEFENDANT.

06CVH-05-6041
CASE NUMBER

CLERK'S ORIGINAL CASE SCHEDULE

	LATEST TIME OF OCCURRENCE
CASE FILED	05/05/06
INITIAL STATUS CONFERENCE	********
INITIAL JOINT DISCLOSURE OF ALL WITNESSES	09/22/06
SUPPLEMENTAL JOINT DISCLOSURE OF ALL WITNESSES	11/17/06
TRIAL CONFIRMATION DATE	12/01/06
DISPOSITIVE MOTIONS	02/09/07
DISCOVERY CUT-OFF	02/23/07
DECISIONS ON MOTIONS	04/06/07
FINAL PRE-TRIAL CONFERENCE/ORDER (OR BOTH)	05/14/07 0845AM
TRIAL ASSIGNMENT	06/06/07 0900AM

NOTICE TO ALL PARTIES

ALL ATTORNEYS AND PARTIES SHOULD MAKE THEMSELVES FAMILIAR WITH THE COURT'S LOCAL RULES, INCLUDING THOSE REFERRED TO IN THIS CASE SCHEDULE. IN ORDER TO COMPLY WITH THE CLERK'S CASE SCHEDULE, IT WILL BE NECESSARY FOR ATTORNEYS AND PARTIES TO PURSUE THEIR CASES VIGOROUSLY FROM THE DAY THE CASES ARE FILED. DISCOVERY MUST BE UNDERTAKEN PROMPTLY IN ORDER TO COMPLY WITH THE DATES LISTED IN THE RIGHT-HAND COLUMN.

BY ORDER OF THE COURT OF COMMON PLEAS,
FRANKLIN COUNTY, OHIO

__/__/__
DATE

JOHN O'GRADY, CLERK

(CIV363-S10)

COURT OF COMMON PLEAS
FRANKLIN COUNTY, OHIO

Tracy L. Key, individually and on behalf of all others similarly situated **20415 Alpine Drive** **Lawrenceburg, Indiana 47025,** **Plaintiffs,** **-vs-** **DSW, Inc.** **4150 East 5th Avenue** **Columbus, Ohio 43219** **c/o CSC-Lawyers Incorporating Service** **50 W. Broad Street, Suite 1800** **Columbus, OH 43215,** **Defendant.**	:	**CASE NO.:** _____ 06 CV H05 6041 **Judge:** _____ **CLASS ACTION COMPLAINT**

FILED
COMMON PLEAS COURT
FRANKLIN CO. OHIO
06 MAY -5 PM 4:41
CLERK OF COURTS-CV

Plaintiff, by her undersigned attorneys for this Class Action Complaint (the "Complaint"), alleges upon personal knowledge as to herself and her own actions, and upon information and belief, as to all other matters, as to which allegations she believes substantial evidentiary support will exist after a reasonable opportunity for further investigation and discovery, as follows:

I. NATURE OF THIS ACTION

1. Between November 2004 and March 2005, Defendant DSW, Inc. ("DSW"), collected and maintained credit card, debit card, and checking account numbers and other confidential personal financial information about approximately 1.5 million consumers who purchased merchandise at DSW retail outlets. As a result of DSW's improper retention of and failure to secure this confidential personal financial information, on or about March 2005,

unauthorized persons obtained access to and acquired confidential and sensitive personal financial information including the credit card and debit card numbers, and related information, of approximately 1.4 million customers, and the checking account numbers, and related information, such as driver license numbers, of approximately 96,000 customers. As a result of this disclosure, Plaintiff and the Class have been subjected to a substantially increased risk of identity theft and have incurred the cost and inconvenience of, among other things, canceling credits cards, closing checking accounts, ordering new checks, obtaining credit reports and purchasing identity and/or credit monitoring.

2. This is a class action on behalf of the approximately 1.5 million consumers who, as a result of Defendant's misconduct, have been subjected to the disclosure and dissemination of confidential personal financial information, including, but not limited to, *inter alia* credit card, debit card and checking account numbers.

II. PARTIES

3. Plaintiff Tracy Key is an adult resident of Lawrenceburg, Indiana who, during relevant times, made retail purchases from DSW in Ohio and who has been notified by DSW that her personal and confidential personal financial information was among the information wrongfully disclosed and/or disseminated as a result of the acts and or omissions of DSW.

4. Defendant DSW, Inc. is an Ohio corporation with its principal office located at 4150 East Fifth Avenue, Columbus, Ohio 43219. DSW does substantial business in Ohio, including Franklin County, and throughout the United States, and therefore is subject to this Court's personal jurisdiction.

III. JURISDICTION

5. This Court has jurisdiction over the parties because DSW is an Ohio corporation that maintains its principal place of business in Ohio. Furthermore, most of the events, actions, inactions, decisions and wrongful conduct complained of herein on the part of DSW occurred in Ohio and/or were originated and controlled from Ohio.

6. Additionally, DSW's executive offices, investor relations, and human resources are all located in Ohio, and DSW maintains a 660,000 square foot distribution center in Ohio.

7. Plaintiff Tracy Key made purchases from DSW in Ohio between November 2004 and March 2005.

8. Venue is proper in Franklin County, Ohio because Defendant conducted extensive and ongoing business activity in Franklin County, Ohio that gave rise to the claims for relief.

9. In this Complaint, Plaintiff asserts no federal question and/or violations of federal laws.

IV. STATEMENT OF THE CASE

10. DSW sells footwear and other merchandise at approximately 199 retail stores in 32 states. At the time of sale of its merchandise in the retail stores, DSW accepts cash, credit cards, debit cards, and personal checks from customers.

11. To process retail purchases with credit cards and debit cards, DSW collects, records, and retains confidential personal financial information from each customer, including name, card number, and expiration date. To process personal check purchases, DSW collects, records, and retains the routing number, account number, check number, the driver license number, and the state of issue. The information DSW collects, records, and retains in connection

with credit card, debit card, and personal check purchases is collectively referred to as "Confidential Personal Financial Information."

12. For a credit or debit card purchase, DSW typically collects the Confidential Personal Financial Information from the magnetic strip of the credit or debit card. The information collected from the magnetic strip includes a security code used to verify electronically that the card is genuine. This code is particularly sensitive because it can be used to create counterfeit credit and debit cards that appear genuine in the authorization process. For purchases using a check, DSW typically collects information from the check using Magnetic Ink Character Recognition technology. In each case, DSW collects the information at the cash register and wirelessly transmits the information, formatted as an authorization request, to a computer network located in the store. The authorization request is then transmitted back to DSW through the same networks. Until at least March 2005, DSW stored Confidential Personal Financial Information used to obtain credit card, debit card, and check authorizations, including magnetic strip data, on in-store and corporate computer networks.

13. DSW operates wireless access points through which the cash registers connect to the in-store computer networks. Other wireless access points are used to transmit information about defendant's inventory from in-store scanners to the in-store computer networks.

14. The Confidential Personal Financial Information constitutes personal property of customers, and when this information is obtained by identity thieves, counterfeiters, or others, the information is unlawfully utilized through a myriad of illegal artifices and schemes, resulting in financial loss to the customers, including unauthorized use of credit cards and withdrawals from checking accounts.

Identity Theft

15. According to the Federal Trade Commission, "Once identity thieves have your personal information, they use it in a variety of ways:

- They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem;
- They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report;
- They may establish phone or wireless service in your name;
- They may open a bank account in your name and write bad checks on that account;
- They may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account;
- They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction;
- They may buy a car by taking out an auto loan in your name;
- They may get identification such as a driver's license issued with their picture, in your name;
- They may get a job or file fraudulent tax returns in your name; or
- They may give your name to the police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name."

See http://www.consumer.gov/idtheft/con_about.htm.

16. In fact, the Federal Trade Commission issued a "FTC Consumer Alert" in March, 2005 titled "What To Do If Your Personal Information Has Been Compromised," which is

available at http://www.ftc.gov/bcp/conline/pubs/alerts/infocompalrt.htm. In this Alert, the FTC warned that "If the stolen information includes your financial accounts, close compromised credit card accounts immediately." The FTC further urged that "If the stolen information includes your driver's license or other government-issued identification, contact the agencies that issued the documents and follow their procedures to cancel a document and get a replacement. Ask the agency to flag you to keep anyone else from getting a license or other identification document in your name." The FTC also instructed that individuals whose personal information has been compromised should "read your financial account statements promptly and carefully, and...monitor your credit reports every few months for the first year of the theft, and once a year thereafter."

17. In a similar publication, titled "Facts for Business- Information Compromise and the Risk of Identity Theft: Guidance for Your Business," (issued in June, 2004 and available at http://www.ftc.gov/bcp/conline/pubs/buspubs/idtrespond.htm), the FTC emphasized that "Potential victims of a theft also should review their credit reports periodically to keep track of whether their information is being misused. For some victims, weeks or months may pass between the time information is stolen and the time it is misused."

18. As a result of the foregoing, it is well established and widely accepted that the failure to implement reasonable and prudent measures to secure Confidential Personal Financial Information collected from retail customers in connection with credit card, debit card, and personal check transactions creates a serious and known risk of harm to such individuals.

19. In recognition of the dangers posed by the disclosure of its customers' Confidential Personal Financial Information, DSW issued and posted a press release on its website, available at http://www.dswshoe.com/credit_card_faq.jsp, that admitted the following:

"We cannot know if the stolen checking account data will or will not be used by the thieves to commit fraud. For this reason, we are providing the following immediate steps (as suggested by the Federal Trade Commission) that you should take to protect your accounts and your personal information. It is important that you take all necessary steps to protect your bank accounts and personal information in light of this theft.

- **Telephone your bank immediately.**
  1. Ask your bank whether you should close those accounts associated with the MICR number and stop payment on all outstanding checks that you do not recognize as yours.

  2. Verify all recent transactions. Ask your bank to provide you with a record of all recent transactions on the bank account that is associated with the stolen MICR number. If unauthorized transactions are identified, ask your bank how to begin the fraud dispute process.

  3. Ask your bank to notify their check verification company of the MICR theft and the stop payment order.

- **Call your state DMV.** Call the office of the Department of Motor Vehicles (DMV) to see if another driver's license was issued in your name. Put a fraud alert on your driver license if your state's DMV provides a fraud alert process. Go to your local DMV to request a new license number. You may have to fill out the DMV's complaint form to begin the investigation process.

- **Obtain your consumer report.** Request a free copy of your consumer report from Chex Systems, Inc. to determine if new accounts have been opened in your name.

  Chex Systems, Inc.
  Attn: Customer Relations
  7805 Hudson Rd., Suite 100
  Woodbury, MN 55125
  1-800-428-9623

- **Obtain your credit report and place a "fraud alert."** Call one of the following Credit Reporting Bureaus to put a "fraud alert" and "victim's statement" on your credit file and request a copy of your credit report (we have provided additional information about

credit reports on our website at http://www.dswshoe.com). Save this letter so, if necessary, you can provide it as proof that you have reason to believe you could be the victim of identity theft.

Equifax: P.O. Box 105069, Atlanta, GA 30348.
Report fraud: Call (800) 525-6285 and write to the address above.
Order a credit report: (800) 685-1111.
TDD: (800) 255-0056
Web: www.equifax.com

Experian (formerly TRW): P.O. Box 9532 Allen, TX 75013.
Report fraud: Call (888-397-3742) and write to address above.
Order credit report: (888) EXPERIAN.
TDD: Use relay to fraud number above.
Web: www.experian.com

TransUnion: P.O. Box 6790, Fullerton, CA 92834.
Report fraud: (800) 680-7289 and write to address above.
Order credit report: (800) 888-4213.
TDD: (877) 553-7803
E-mail (fraud victims only): fvad@transunion.com
Web: www.transunion.com

- **Report any crimes to your local police.** If the information that you have gathered from your bank, the DMV, the check verification company and/or the credit reporting bureaus demonstrate that someone has been illegally using your account number or driver's license number, you should report the crime to your local police or sheriff's department. Give the law enforcement agency as much documented evidence as possible and make sure the police report lists the fraudulent accounts. Get a copy of the police report, keep the phone number of your investigator handy and give it to creditors and others who require verification of your case.

- **File your case with the Federal Trade Commission.** In addition, if you discover that someone has been illegally using your account number or driver's license number, you may wish to file your case with the Federal Trade Commission to help national law enforcement agencies track and stop identity thieves. The Federal Trade Commission also provides an Identity Theft Affidavit at its web site. Completion of this Affidavit could assist you when disputing unauthorized accounts with creditors. To file your case with the FTC Consumer Response Center or obtain an Identity Theft Affidavit, call 1- (877) IDTHEFT (877-438-4338), or visit www.consumer.gov/idtheft."

20. In sum, DSW's failure to protect and secure the Confidential Personal Financial Information collected from retail customers in connection with credit card, debit card, and personal check transactions has created an actual and grave risk of injury to these customers.

DSW's Conduct

21. Until approximately March or April 2005, DSW collected Confidential Personal Financial Information of its retail customers at the cash register and wirelessly transmitted the information, formatted as an authorization request, to a computer network located in the store. The authorization request was then transmitted back to DSW through the same networks. Until at least March 2005, DSW stored Confidential Personal Financial Information used to obtain credit card, debit card, and check authorizations, including magnetic stripe data, on in-store and corporate computer networks.

22. Also until approximately March or April 2005, DSW operated wireless access points through which the cash registers connected to the in-store computer networks. Other wireless access points were used to transmit information about defendant's inventory from in-store scanners to the in-store computer networks.

23. The Federal Trade Commission, pursuant to its statutory authority, has promulgated regulations with respect to the handling of Confidential Personal Financial Information by those within its jurisdiction, including without limitation Parts 314 and 682 of Title 16 of the Code of Federal Regulations regarding "Standards for Safeguarding Customer Information" and "Disposal of Consumer Report Information and Records." These standards represent a recognition of the financial dangers posed to the public by the mishandling of Confidential Personal Financial Information and require covered entities to, among other things, "insure the security and confidentiality of customer information," "protect against any

anticipated threats or hazards to the security or integrity of such information," "protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer," and "properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal."

24. Consistent with the foregoing standards, financial institutions require all merchants who desire to accept payment by credit cards, including Defendant DSW, to abide by certain standards with respect to the collection and maintenance of Confidential Personal Financial Information as a condition of doing business with major credit card companies, including without limitation Visa, Mastercard, American Express, and Discover. These standards are well established and widely accepted and understood in the retail industry and generally require secure storage of Confidential Personal Financial Information and limit retention to such time as the data is required for a bona fide purpose.

25. At all relevant times, DSW employed several practices which failed to abide by the aforementioned standards and failed to protect from disclosure the Confidential Personal Financial Information it collected from its customers. Such failures included that DSW: (1) created unnecessary risks of the disclosure of Confidential Personal Financial Information by permanently retaining it in multiple files when it no longer had a legitimate business need for the Confidential Personal Financial Information; (2) failed to implement readily available and commercially reasonable and prudent security measures to limit access to its computer networks containing Confidential Personal Financial Information via wireless access points accessible in and around DSW's stores; (3) stored Confidential Personal Financial Information in unencrypted files that could be easily accessed by using a commonly known user ID and password; (4) failed

to limit the ability of in-store computer networks to be used to access other networks containing Confidential Personal Financial Information; (5) failed to implement readily available and commercially reasonable and prudent measures to detect and limit unauthorized access to computer networks containing Confidential Personal Financial Information or through which such information could be accessed.

26. As a direct and proximate result of DSW's failure to protect its customers' Confidential Personal Financial Information, sometime after mid-February 2005, unauthorized individuals were able to obtain computer files from DSW containing the Confidential Personal Financial Information of approximately 1.5 million customers. These files included approximately 1.4 million credit and debit card files and 96,000 checking account and driver license numbers.

27. As set forth above, DSW's failure to protect its customers' Confidential Personal Financial Information resulted in fraudulent charges on some customers' debit, credit and/or checking accounts. Also as a direct and proximate result of DSW's failure to adequately or reasonably protect its customers' Confidential Personal Financial Information, all customers whose information was wrongfully disclosed have been exposed to a substantial increase in the risk of being a victim of identity theft or other financial crime.

28. In March 2005, DSW issued a press release confirming the loss of its customers' Confidential Personal Financial Information from 108 stores in 25 states. At approximately the same time, DSW began notifying some (but not all) affected customers that their Confidential Personal Financial Information was among that disclosed as a result of DSW's failures. A true and accurate copy of the letter received by Plaintiff is attached as Exhibit A. Among other things, DSW advised affected customers to contact their banks and consult the FTC about how to

protect themselves from identity theft. As a direct and proximate result, members of the proposed class have incurred the cost and inconvenience of, among other things, canceling credits cards, closing checking accounts, obtaining credit reports, and purchasing identity and/or credit monitoring services.

29. Recent studies confirm that, on average, victims of identity theft incur significant tangible losses of personal time sometimes ranging in the hundreds of hours and out-of-pocket expenses averaging hundreds of dollars. *See, e.g.*, Identity Theft: The Aftermath 2003, available at www.idtheftcenter.org.

30. Yet, despite the overall substantial costs and inconveniences due to DSW's failures and the resulting security breach, DSW spokesman Rob Whitehouse stated in an interview with the AARP Bulletin that DSW had no plans to compensate customers for personal expenses, such as ordering new checks. "We feel that many charges will be reimbursed through banks or credit card companies." *See* AARP Bulletin: Trouble Afoot: The DSW Security Breach, June 2005, available at www.aarp.org/bulletin/consumer/dsw_security_breach.html.

V. CLASS ACTION ALLEGATIONS

31. Plaintiff brings all claims herein as class claims pursuant to Civ. R. 23. The requirements of Rule 23 (A) and (B)(2) are met with respect to the class defined below.

A. Class Definition

32. Consumers who made retail purchases from DSW between November 2004 and March 2005 by means of a credit card, debit card, or personal check, and whose Confidential Personal Financial Information was obtained via a breach of DSW's computer system(s), customer database(s), and/or means or system which serves to retain and/or store customers'

Confidential Personal Financial Information. Excluded from this class are Defendant's corporate officers, directors, and employees.[1]

B. Numerosity

33. At this time, Plaintiff does not know the exact size of the Class; however, Defendant has publicly admitted that approximately 1.4 million customers had their credit and debit card information stolen, and that approximately 96,000 customers had their checking account numbers and related information stolen. As such, Plaintiff believes that the class members are so numerous that joinder of all members is impracticable

C. Commonality

34. There are questions of law or fact common to the Class, including at least the following:

a. whether DSW failed to adequately protect its customers' Confidential Personal Financial Information;

b. whether DSW engaged in unlawful and tortious conduct;

c. whether DSW's conduct was willful and/or reckless;

d. whether DSW was negligent in allowing the disclosure of Confidential Personal Financial Information by failing to exercise due care to protect the Confidential Personal Financial Information it collected, recorded, and maintained in view of the known risks of identity theft to customers created by such a failure;

e. whether DSW should be required to notify each and every affected customer whose Confidential Financial Information was misappropriated as a result of DSW's acts and omissions; and

[1] Plaintiff reserves the right to request revisions to the class definition pursuant to Ohio Civ. R. 23(C)(1) as discovery is completed in this action.

f. whether DSW should be required to take remedial protective measures for the benefit of the Class, including providing the Class with identity and/or credit monitoring program and pre-emptive internet search service due to the actual and ongoing threat of identity theft to the Class caused by DSW's acts and omissions.

D. Typicality

35. Plaintiff has the same interests in this matter as all other members of the Class, and her claims are typical of all members of the Class.

E. Adequacy

36. Plaintiff is committed to pursuing this action and has retained competent counsel experienced in class actions. Plaintiff will fairly and adequately represent the interests of the Class and does not have interests adverse to the Class. Plaintiff specifically reserves the right to add additional class representatives as necessary.

F. The Prerequisites to Maintaining a Class Action For Injunctive and Corresponding Declaratory Relief Pursuant to Civ. R.23(B)(2) Are Readily Apparent

37. A class certified for injunctive relief is appropriate because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive and equitable relief with respect to the Class as a whole.

38. Defendant's actions are generally applicable to the Class as a whole, and Plaintiff seeks, *inter alia*, equitable remedies with respect to the Class as a whole.

39. Defendant's systemic policies and practices make declaratory relief with respect to the Class as a whole appropriate.

40. A reparative injunction mandating appropriate remedial measures to protect against and prevent the future harmful effects of Defendant's past acts, including an identity and/or credit monitoring program and a pre-emptive internet search service, is proper for Plaintiff and the Class on a court-appointed, court-supervised basis. Such an injunction is

necessary to restore Plaintiff and the Class to the status quo that existed prior to DSW's failures, actions, and inactions that resulted in the theft of Class Members' Confidential Personal Financial Information.

G. The Class Action Device Is Proper

41. The likelihood that individual members of the Class will prosecute separate actions is remote due to the extensive time and considerable expense necessary to conduct such litigation, especially in view of the relatively modest amount of monetary, injunctive, and equitable relief at issue for each individual class member. This action will be prosecuted in a fashion to ensure the Court's able management of this case as a class action.

42. The application of Ohio law to the class members of the 25 states affected by this action is appropriate because DSW is an Ohio corporation that is incorporated in Ohio and has its principal and centralized place of business operations in Ohio. DSW investor relations, human resources, and the executive offices are all in Columbus, and DSW's first store was in Dublin, Ohio. Most of the events, actions, decisions, and transactions complained of herein occurred in Ohio and were originated and controlled from Ohio. Thus, there is a meaningful nexus and significant connection and contact between the State of Ohio and the conduct under dispute. Thus, this Court, as a branch of the government of the State of Ohio, and Ohio as a forum state have a strong judicial, governmental, and policy interest in ensuring that the wrongful conduct and Ohio law violations complained of are addressed before this Court under Ohio law.

VI. STATEMENT OF CLAIMS

COUNT I

Ohio Consumer Sales Practices Act

43. Plaintiff incorporates paragraphs 1 through 42 herein above.

44. Plaintiffs' first cause of action seeks all appropriate relief pursuant to DSW's unfair and/or or deceptive consumer sales practices towards the Class.

45. DSW is and was at all times material hereto a supplier as that term is defined in R.C. 1345.01(C). Specifically, DSW is and was engaged in the business of effectuating "consumer transactions" by soliciting and selling goods and services to consumers for purposes that are primarily personal, family, or household within the meaning of R.C. 1345.01(A) and (D).

46. DSW collected, utilized, and retained Confidential Personal Financial Information in connection with, as a part of, and in order to effectuate "consumer transactions."

47. DSW's failure to properly collect, utilize, and retain Confidential Personal Financial Information and to protect such information from disclosure constitutes an unfair and deceptive act or practice in violation of Ohio's Consumer Sales Practices Act, R.C. 1345.02(A) and an unconscionable practice under R.C. 1345.03.

48. As a direct and proximate result of Defendants' violation of O.R.C. §1345.02 and §1345.03, Plaintiff and the Class have been subjected to a substantial increase in their risk of identity theft or other related financial crimes.

COUNT II

Negligence

49. Plaintiff incorporates paragraphs 1 through 48 herein above.

50. Plaintiff's second cause of action seeks all appropriate relief pursuant to DSW's negligence towards the Class.

51. DSW owed Plaintiff and the Class a duty to exercise reasonable care, skill, and faithfulness with respect to the collection, use, transmission, and retention of the Confidential Personal Financial Information. The high degree of imminent danger posed by the disclosure of

Confidential Personal Financial Information was well known before and at the time of the events giving rise to this Complaint. As a result, ordinary and reasonable prudence mandates a high degree of care in the collection, use, transmission, and retention of Confidential Personal Financial Information.

52. DSW breached its duty of care to Plaintiff and the Class as alleged above.

53. As a direct, proximate, and foreseeable result of DSW's breach of its duty, Plaintiff and the Class have been injured. Injuries include, but are not limited to, class members incurring expenses and suffering inconvenience and aggravation associated with closing accounts and opening new accounts, obtaining credit reports, and purchasing credit and/or identity monitoring. As a direct and proximate result of DSW's negligence, Plaintiff and the Class have been subjected to a substantial increase in their risk of identity theft or other related financial crimes.

COUNT III

Breach of Contract Implied-In-Fact

54. Plaintiff incorporates paragraphs 1 through 53 herein above.

55. Plaintiff's third cause of action seeks all appropriate relief pursuant to DSW's Breach of Contract Implied-In-Fact.

56. Plaintiff and the Class purchased merchandise from DSW using credit cards, debit cards, and/or checks during the relevant time period.

57. In making these purchases, Plaintiff and the Class necessarily entrusted Confidential Personal Financial Information to DSW, including (1) for credit card purchasers the customer's name, card number, and expiration date, (2) for debit card purchasers the customer's name, card number and account number, and (3) for personal check purchasers, the routing

number, account number, check number and the customer's driver license number and the state of issue.

58. An implied-in-fact contract between Plaintiff and the Class and DSW existed through a tacit understanding that if Plaintiff and the Class made a retail purchase from DSW using a credit card, debit card, or personal check, DSW would protect the Confidential Personal Financial Information from being accessed by, or disclosed to, unauthorized persons.

59. Because of this understanding, Plaintiff and the Class entrusted DSW with their Confidential Personal Financial Information.

60. In the absence of this understanding, Plaintiff and the Class would not have entrusted DSW with this Confidential Personal Financial Information.

61. By retaining and storing the Confidential Personal Financial Information of Plaintiff and the Class, and by failing to protect this information so as to prevent access by, or disclosure to, unauthorized parties, DSW has breached its contractual obligations to Plaintiff and the Class.

62. As a direct, proximate, and foreseeable result of DSW's breach of its implied-in-fact contract with Plaintiff and the Class, Plaintiff and the Class have been subjected to a substantial increase in their risk of identity theft or other related financial crimes.

COUNT IV

Conversion

63. Plaintiff incorporates paragraphs 1 through 62 herein above.

64. Plaintiff's fourth cause of action seeks all appropriate relief pursuant to DSW's Conversion.

65. By unnecessarily retaining and storing the Confidential Personal Financial Information of Plaintiff and the Class, and by failing to protect this information so as to prevent access by, or disclosure to, unauthorized parties, DSW wrongfully exercised dominion and control over Plaintiff and the class members' personal property in a manner inconsistent with the rights of Plaintiff and the Class.

66. As a direct, proximate, and foreseeable result of DSW's conversion of the personal property of Plaintiff and the Class, Plaintiff and the Class have been subjected to a substantial increase in their risk of identity theft or other related financial crimes. Further, Plaintiff and the Class are entitled to recover punitive damages as a result of DSW's malicious conduct evidenced by a callous and conscious disregard for the rights of Plaintiff and the Class.

COUNT V

Breach of Fiduciary Duty

67. Plaintiff incorporates paragraphs 1 through 66 herein above.

68. Plaintiff's fifth cause of action seeks all appropriate relief pursuant to DSW's Breach of Fiduciary Duty.

69. At the time Plaintiff and the Class gave DSW access to the Confidential Personal Financial Information in connection with their retail purchases, a special confidence and trust was necessarily reposed in the integrity and fidelity of DSW by Plaintiff and the Class.

70. By virtue of this special trust, DSW acquired a position of superiority and/or influence over the Confidential Personal Financial Information of Plaintiff and the Class.

71. Also by virtue of this special trust, DSW had a special duty to act for the benefit of Plaintiff and the Class by protecting the Confidential Personal Financial Information of

Plaintiff and the Class in a fashion so as to prevent access by, or disclosure to, unauthorized persons or entities.

72. By failing to secure the Confidential Personal Financial Information of Plaintiff and the Class so as to prevent access by, or disclosure to, unauthorized parties, DSW breached its fiduciary duty.

73. As a direct, proximate, and foreseeable result of DSW's breach of its fiduciary duty to Plaintiff and the class members, Plaintiff and the Class have been subjected to a substantial increase in their risk of identity theft or other related financial crimes.

COUNT VI

Breach of Contract- Third Party Beneficiary

74. Plaintiff incorporates paragraphs 1 through 73 herein above.

75. Plaintiffs' sixth cause of action seeks all appropriate relief pursuant to DSW's Defendant's Breach of Contract.

76. Upon information and belief, DSW executed an agreement to comply with the Bylaws and Rules set forth in MasterCard International Incorporated's Merchant Rules Manual, as well as substantially similar agreements with Visa, American Express and Discover (see Exhibit B).[2]

77. The MasterCard Merchant Rules Manual, and the substantially similar agreements issued by Visa, American Express and Discover, are valid and legally binding agreements.

78. These bylaws and rules require that DSW, as a merchant, must not unnecessarily retain or store Cardholder information after a transaction has been authorized.

[2] Exhibit B contains the relevant portions of the agreement between Mastercard and DSW. The entire agreement is over 200 pages long and is not attached in its entirety. Nonetheless, upon information and belief, the parties have a complete copy of this agreement.

79. DSW did unnecessarily retain and store Cardholder information in violation of the agreements.

80. These bylaws and rules also require that DSW, as a merchant, must keep all systems and media containing Cardholder information in a secure manner so as to prevent access by, or disclosure to any unauthorized party.

81. DSW did not keep the Cardholder information secure and as such, allowed unauthorized parties to obtain access to it.

82. Plaintiff and the classes are third party beneficiaries of MasterCard's Merchant Rules Manual, and other similar agreements with Visa, American Express and Discovery.

83. By retaining and storing Cardholder information that was not necessary for any bona fide purpose, and by failing to secure Cardholder information to prevent access by, or disclosure to, unauthorized parties, DSW has breached its obligations to Plaintiff and the classes as third party beneficiaries of DSW's agreements with MasterCard, Visa, American Express and Discovery.

84. As a direct, proximate, and foreseeable result of DSW's breach of its obligations under the Merchant Rules Manual and other substantially similar agreements, Plaintiff and the Class have been subjected to a substantial increase in their risk of identity theft or other related financial crimes.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on her own behalf, and on behalf of the Class, prays for relief as follows:

1. An order certifying this action as a class action under Civ. R. 23(B)(2) and appointing Plaintiff and her undersigned counsel to represent the Class;

2. An reparative injunction requiring Defendant to take necessary measures to safeguard against the grave harm attendant to the improper disclosure/ theft of the Confidential Personal Financial Information, including an identity and/or credit monitoring program and a pre-emptive internet search service for the benefit of Plaintiff and the Class under this Court's supervision;

3. An order requiring Defendant to take necessary measures to notify each and every affected customer whose Confidential Personal Financial Information was misappropriated as a result of DSW's acts and omissions;

4. An award of punitive damages for DSW's malicious conduct;

5. An award of attorneys' fees; and

6. Such other and further relief as this Court may deem just, equitable or proper.

Respectfully submitted,

John C. Murdock per written authority 5/5/06 cjw

JOHN C. MURDOCK (0063749)
JEFFREY S. GOLDENBERG (0063771)
TODD B. NAYLOR (0068388)
MURDOCK GOLDENBERG SCHNEIDER & GROH, L.P.A.
35 East Seventh Street, Suite 600
Cincinnati, Ohio 45202-2446
Telephone: (513) 345-8291
Facsimile: (513) 345-8294

Christian Jenkins per written authority 5/5/06 cjw

MARC D. MEZIBOV (0019316)
CHRISTIAN A. JENKINS (0070674)
STACY C. HINNERS (0076458)
MEZIBOV & JENKINS, CO. L.P.A.
401 East Court Street, Ste. 600
Cincinnati, Ohio 45202
Telephone: (513) 723-1600
Facsimile: (513) 723-1620

Elizabeth J. Watters (0054055)
Charles R. Saxbe (0021952)
David J. Butler (0068455)
CHESTER WILLCOX & SAXBE, LLP
65 East State Street, Ste. 1000
Columbus, Ohio 43215
Telephone: (614) 221-4000
Facsimile: (614) 221-4012

Trial Attorneys for Plaintiff Tracey Key

DSW

Tracy L. Key
20415 Alpine Dr
Lawrenceburg, IN 47025-9345

MASTERCARD 5174

Dear Tracy L. Key:

As you may have read or seen in local or national media reports, DSW was the victim of a significant theft of customer data including credit card and debit card numbers. In the last few weeks, we have investigated this theft and taken every step we can to prevent further data theft of this nature. Within days of our discovery of this theft, we provided the stolen credit and debit card numbers to American Express, Discover, VISA and MasterCard. We have confirmed that VISA and MasterCard provided these card numbers to the appropriate issuing banks (these are the banks that issue cards to people like you).

As a merchant accepting credit cards, we do not collect the addresses of the cardholders when purchases are made. However, we did subsequently determine that many of the affected cardholders were also Reward Your Style (RYS) customers for whom we had addresses. Thus, while it took additional time to match our files, we are writing to you because you are a valued RYS customer and we have now verified that your credit card or debit card was among the customer information that was stolen. **For your convenience, we have included in the upper right corner of this page the credit card type and last 4 digits of the credit card that was affected. If you had multiple cards affected, they are all listed.** We do not collect PIN numbers for debit cards, so if your debit card information was taken, the PIN was not stolen. We also want to assure you that your RYS information was not stolen. We deeply regret that this theft of data from DSW might also make you a possible victim of the fraudulent use of your credit card or debit card.

We cannot know if your credit card or debit card will or will not be used by the thieves to commit a fraud. We would first suggest that you contact the bank that issued your card (the phone number should be on the back of your credit card) and follow the procedures that they recommend. To assist our customers who have been affected by this theft, we have provided information about steps that can be taken, how to obtain a credit report, and FAQs on our website at http://www.DSWshoe.com. The Federal Trade Commission also provides detailed information to consumers on these issues and can be contacted at 1-877-438-4338 or http://www.consumer.gov/idtheft/. Finally, we would recommend that you save this letter so, if necessary, you can provide it as proof that you have reason to believe you are a victim of this theft.

We want to emphasize once again that within days of the discovery of the theft, DSW provided the stolen credit and debit card numbers to American Express, Discover, VISA and MasterCard, which then provided those numbers to the issuing banks.

We greatly regret the inconvenience this incident may cause you. We are taking this issue very seriously and will work with the authorities to pursue those responsible for this crime and prosecute them to the fullest extent of the law.

Sincerely,

Debbie Ferree

Debbie Ferree
President

960050

Corporate Offices: 4150 East Fifth Avenue, Columbus, OH 43219
DSWshoe.com

EXHIBIT
A

Information about this Replacement

Replacement

The March 2005 *Merchant Rules Manual* replaces your existing manual.

Contents

This manual contains excerpts of MasterCard member publications that provide information about standards applicable to MasterCard merchants.

Questions?

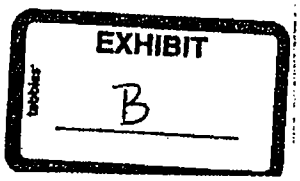
If you have questions about this manual, please contact the Customer Operations Services team or your regional help desk. If you are a merchant, please contact your acquirer.

MasterCard is Listening...

Please take a moment to provide us with your feedback about the material and usefulness of the *Merchant Rules Manual* using the following e-mail address:

publications@mastercard.com

We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.



Merchant Rules Manual

March 2005

Copyright

The information contained in this manual is proprietary to MasterCard International Incorporated (MasterCard) and its members.

Trademarks

Trademark notices and symbols used in this manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Media

This document is available via the following Web sites:

- MasterCard OnLine®
- www.mastercardmerchant.com

MasterCard International Incorporated
2200 MasterCard Boulevard
O'Fallon MO 63366-7263
USA

1-636-722-6100

www.mastercard.com

Chapter 1 Overview

Chapter 2 Excerpts from *Bylaws and Rules* (published October 2004)

© 2005 MasterCard International Incorporated

Table of Contents

© 2005 MasterCard International Incorporated

© 2005 MasterCard International Incorporated

© 2005 MasterCard International Incorporated

Chapter 4 Excerpts from *GCMS Reference Manual* (published December 2004)

Chapter 5 Excerpts from *Security Rules and Procedures* (published January 2005)

© 2005 MasterCard International Incorporated

© 2005 MasterCard International Incorporated

© 2005 MasterCard International Incorporated

Table of Contents

© 2005 MasterCard International Incorporated

© 2005 MasterCard International Incorporated

Table of Contents

© 2005 MasterCard International Incorporated

© 2005 MasterCard International Incorporated

Table of Contents

© 2005 MasterCard International Incorporated

9.14.2 Present Transactions within Three Business Days

The merchant must present records of valid transactions to its acquirer no later than three bank business days after the date of the transaction, except

- the record must not be presented until after the goods are shipped or the services are performed unless, at the time of the transaction, the cardholder agrees to a properly disclosed delayed delivery of the goods or services,
- when the merchant receives authorization for a delayed presentment (in which case the words "Delayed Presentment" must be noted on the TID),
- when the merchant is obligated by law to retain the sales slip or return it to a buyer upon timely cancellation, in which case the merchant should present the record within 10 business days after the transaction date, and
- when the merchant has multiple locations and uses a central facility to accumulate and present records to the acquirer. In this case, the merchant must present the record in accordance with applicable laws and regulations and, in any event, within 30 days of the transaction date.

9.15 Account, Cardholder, Transaction, and Merchant Information

9.15.1 Sale or Exchange of Account and Cardholder Information Prohibited

A merchant must not sell, purchase, provide, exchange or in any manner disclose MasterCard account number information to anyone other than its acquirer, to the Corporation, or in response to a government request. This prohibition applies to card imprints, transaction receipts, carbon copies, mailing lists, tapes, or other media obtained as a result of a MasterCard card transaction.

9.15.2 Fraudulent or Unauthorized Use of Account Information Prohibited

A merchant must not request or use MasterCard account number information for any purpose that it knows or should have known to be fraudulent or in violation of MasterCard Standards, or for any purpose that the cardholder did not authorize.

© 2005 MasterCard International Incorporated

9.15.3 Account, Cardholder and Transaction Data Must Be Kept Secure

Merchants and DSEs must keep all systems and media containing MasterCard account, cardholder, or transaction information (whether physical or electronic) in a secure manner so as to prevent access by, or disclosure to any unauthorized party. Merchants and DSEs must destroy all media not necessary to retain, in a manner that will render the data unreadable. Only MasterCard account, cardholder, and transaction information may be stored, and then only to the extent permitted by the Standards.

If an account compromise occurs, the following will apply:

- The merchant must notify the acquirer immediately.
- The acquirer must provide the Corporation with complete information about the account compromise.
- If the account compromise results from the merchant's failure to comply with this rule, the acquirer promptly must engage a data security firm acceptable to the Corporation to assess the vulnerability of the merchant systems and provide the results of such audit (or a forensics examination if required by MasterCard) promptly to the Corporation.
- If the acquirer fails to engage promptly the services of a data security firm acceptable to the Corporation or fails to provide the findings of the audit, or any forensics examination, promptly to the Corporation, the Corporation may assess the acquirer in accordance with the schedule set forth in section 9.5.2 and may assess all investigative costs that the Corporation incurs.
- The acquirer must cooperate, and ensure that its merchant cooperates, with the investigation and resolution of the account compromise, including any forensic audit or other measure that the Corporation deems necessary in its sole discretion.

Refer to section 5.12 of the *Security Rules and Procedures* manual for additional requirements applicable in the event of account data compromise.

9.15.4 Account Information Must Not Be Recorded on a Mailer

A merchant must not ask a cardholder to record a MasterCard card account number or other account information on the exterior of any order form or other similar device designed to be mailed.

© 2005 MasterCard International Incorporated

9.15.5 Merchant Identification

A merchant must prominently and unequivocally inform the cardholder of the identity of the merchant at all points of interaction so that the cardholder readily can distinguish the merchant from any other party such as a supplier of goods or services to the merchant..

9.15.6 Data Storage Entity (DSE) Identification

The merchant must inform the acquirer promptly of the identity of any DSE that engages, or proposes to engage, in the processing, storage, or both of MasterCard account data for the merchant, whether directly or indirectly, regardless of the manner or duration of such activities.

9.15.7 Storage of Account, Cardholder, and Transaction Data

A merchant and any DSE must not store in any system or in any manner, discretionary card-read data, CVC 2 data, PIN data, Address Verification Service (AVS) data, or any other prohibited information as set forth in the MasterCard Standards including, but not limited to, sections 2.5.5.1.1 and 2.8.2.1 of the Security Rules and Procedures manual, except during the authorization process for a transaction, that is, from the time an Authorization Request message is transmitted and up to the time the Authorization Request Response message is received. MasterCard permits storage of only the card account number, expiration date, cardholder name, and service code, in a secure environment to which access is limited, and then only to the extent that this data is required for bona fide purposes and only for the length of time that the data is required for such purposes.

© 2005 MasterCard International Incorporated

2.5 Card Description

The card has a face and back, each with unique characteristics and requirements. The card face has embossed account information, such as cardholder name, account number, and expiration date. The card back contains a signature panel and a magnetic stripe that contains electronically encoded account information.

2.5.5 Card Back Requirements

2.5.5.1 Magnetic Stripe

2.5.5.1.1 Rules for Disclosure of Card-read Data

The following rules and restrictions apply for the display and storage of card-read data:

- A terminal or other device at the point of interaction must not display, replicate, or store any card-read data except card account number, expiration date, extended service code, and cardholder name, if present.
- The acquirer, the merchant, a data storage entity (DSE), or any agent representative thereof (including third-party processors [TPPs]), may record only the card account number, expiration date, extended service code, and cardholder name on paper, microfiche, or an online authorization file, in a secure environment to which access is limited, solely for research or exception processing purposes at its site. The issuer may request a copy of the data that is retained for such purposes. The acquirer, merchant, DSE, or any agent representative thereof may retain or replicate no other transaction data. Acquirers that currently store full card-read (including discretionary) data for the sole purpose of providing documentation for exception processing must discontinue such storage as soon as practical, but no later than 1 October 2005.

MasterCard strongly recommends that acquirers review their procedures and systems, and those of their merchants, DSEs, agents, and representatives, to ensure compliance with these Standards.

At its discretion, MasterCard may impose a noncompliance assessment for failure to comply with these requirements, as described in section 9.5.2.3 of the *Bylaws and Rules* manual.

© 2005 MasterCard International Incorporated

Definition **Data Storage—The temporary or permanent retention of MasterCard account data in any form (including logs) for subsequent processing, retrieval, or other use.**

MasterCard has sole discretion to interpret and enforce the SDP Program rules.

The MasterCard SDP Program consists of four components:

- MasterCard Security Standard
- Security evaluation tools
- Optional compliance testing process for data security vendors
- Acquirer registration of merchants, TPPs, and DSEs that store account data information

Definition **Data Storage Entity (DSE)—An entity other than a member, merchant, or third-party processor or other MSP that stores MasterCard account data, transaction data, or both. Examples of DSEs include, but are not limited to, Web hosting companies, payment gateways, terminal drivers, software providers, and processors.**

5.13.1 MasterCard Security Standard

The MasterCard SDP Program establishes data security guidelines and requirements specified in the MasterCard Security Standard. The MasterCard Security Standard, although intended for use by e-commerce merchants and TPPs, is applicable to every entity they connect to that has access to and stores account data.

To be compliant with the MasterCard Security Standard, acquirers must ensure that all of these entities adequately safeguard data.The MasterCard Security Standard manuals are available in the Member Publications product of MasterCard OnLine®, as well as on the MasterCard SDP Program Web site at https://sdp.mastercardintl.com.SDP manuals include:

- *Electronic Commerce Requirements and Best Practices for Acquirers*
- *MasterCard Security Standard Applicable to Vendors*
- *MasterCard Security Standard Applicable to Merchants and Member Service Providers*

© 2005 MasterCard International Incorporated

In addition, the *Electronic Commerce Security Architecture Best Practices* document presents architectures, methodologies, and best practices for establishing a secure e-commerce environment.

5.13.2 Security Evaluation Tools

Merchants, TPPs, and DSEs must use two Web site security evaluation tools, the Security Self-assessment and a Network Security Scan, to determine whether these entities are compliant with the MasterCard Security Standard.

The Security Self-assessment is a questionnaire available at no charge on the MasterCard SDP Program Web site at https://sdp.mastercardintl.com.

To be compliant, each e-commerce merchant, TPP, and DSE must, on an annual basis, generate a Security Self-assessment questionnaire with acceptable ratings.

A Network Security Scan evaluates the security measures in place at a Web site.

To fulfill the network scanning requirement, merchants, TPPs, and DSEs must conduct scans in accordance with the requirements set forth in the *MasterCard Security Standard Applicable to Merchants and Member Service Providers*, using a vendor that meets the requirements of the *MasterCard Security Standard Applicable to Vendors*.

5.13.3 Vendor Compliance Testing

As part of the MasterCard SDP Program, MasterCard provides an optional vendor compliance testing process for acquirers that request MasterCard to evaluate the services of a data security firm to ensure compliance with the *MasterCard Security Standard Applicable to Vendors*.

For more information about this service, acquirers should visit the MasterCard SDP Program Web site at https://sdp.mastercardintl.com.

5.13.4 Acquirer Requirements

To ensure compliance with the MasterCard SDP Program, an acquirer must:

- Use the MasterCard SDP Service or engage the services of a third-party security vendor compliant with the *MasterCard Security Standard Applicable to Vendors* for the Network Security Scan Requirement.

© 2005 MasterCard International Incorporated